**İçerik**

| Ders Kodu | Dersin Adı | Yarıyıl | Teori | Uygulama | Lab | Kredisi | AKTS |
|---|---|---|---|---|---|---|---|
| IND465 | Endüstriyel Sistemler için Siber Güvenlik/Dayanıklılık | 7 | 3 | 0 | 0 | 3 | 4 |

| | |
|---|---|
| Ön Koşul | |
| Derse Kabul Koşulları | |

| | |
|---|---|
| Dersin Dili | Fransızca |
| Türü | Seçmeli |
| Dersin Düzeyi | Lisans |
| Dersin Amacı | Geleneksel bilişim (IT) güvenliğinden farklı olarak, üretim sürekliliği ve fiziksel güvenliğin ön planda olduğu Operasyonel Teknoloji (OT) dünyasını güvence altına almayı öğretmek. Mühendislerin siber riskleri yönetme ve tedarik zincirindeki veri zafiyetlerini engelleme kapasitesini geliştirmek. |
| İçerik | o Hafta 1: Siber Güvenliğe Giriş: Bilgi Teknolojileri (IT) vs. Operasyonel Teknolojiler (OT) Paradigması (CIA triad vs. AIC triad).<br>o Hafta 2: Endüstriyel Kontrol Sistemleri (ICS) ve SCADA mimarilerinin zafiyet analizi.<br>o Hafta 3: ICS Tehdit Modellemesi: Tarihsel saldırı vektörleri (Stuxnet, BlackEnergy) ve endüstriyel fidye yazılımları (Ransomware).<br>o Hafta 4: Endüstriyel Ağ Güvenliği: Purdue Referans Modeli ile ağ bölümlendirme (Network Segmentation) ve hava boşluğu (Air-gapping) efsanesi.<br>o Hafta 5: OT İletişim Protokolü Zafiyetleri: Modbus, DNP3 ve Profinet'in güvenlik eksiklikleri ve risk mitigasyonu.<br>o Hafta 6: Endüstriyel Sistemler için Siber Risk Analizi metodolojileri ve zafiyet tarama.<br>o Hafta 7: Ara Sınav.<br>o Hafta 8: Tehdit Algılama: OT ağlarında Saldırı Tespit Sistemleri (IDS) ve anomali tespiti.<br>o Hafta 9: Olaylara Müdahale (Incident Response) ve Felaket Kurtarma (Disaster Recovery) süreçleri.<br>o Hafta 10: İş Sürekliliği Planlaması (Business Continuity Planning - BCP): Kriz anında manuel operasyonlara dönüş senaryoları.<br>o Hafta 11: Tedarik Zinciri Siber Güvenliği: Üçüncü parti satıcı riskleri, donanım truva atları ve sahte (counterfeit) bileşenler.<br>o Hafta 12: Üretimde Sıfır Güven (Zero Trust) Mimarisi: Kimlik doğrulama, erişim kontrolü ve en az yetki prensibi.<br>o Hafta 13: Uluslararası Standartlar ve Uyumluluk: IEC 62443 endüstriyel güvenlik standardı ve NIST Siber Güvenlik Çerçevesi (CSF).<br>o Hafta 14: Siber-Fiziksel Dayanıklılık (Resilience) Mühendisliği: Sistem mimarisini şokları emecek ve hızlı iyileşecek şekilde tasarlama (Vaka analizleri). |
| Kaynaklar | Ders Kitabı: Knapp, E. D., & Langill, J. T. (2014). Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Syngress.<br>Yardımcı Kaynak: Macaulay, T., & Singer, B. (2011). Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS. CRC Press. |

**Teori Konu Başlıkları**

| Hafta | Konu Başlıkları |
|---|---|
| 1 | o Hafta 1: Siber Güvenliğe Giriş: Bilgi Teknolojileri (IT) vs. Operasyonel Teknolojiler (OT) Paradigması (CIA triad vs. AIC triad). |
| 2 | o Hafta 2: Endüstriyel Kontrol Sistemleri (ICS) ve SCADA mimarilerinin zafiyet analizi. |
| 3 | o Hafta 3: ICS Tehdit Modellemesi: Tarihsel saldırı vektörleri (Stuxnet, BlackEnergy) ve endüstriyel fidye yazılımları (Ransomware). |
| 4 | o Hafta 4: Endüstriyel Ağ Güvenliği: Purdue Referans Modeli ile ağ bölümlendirme (Network Segmentation) ve hava boşluğu (Air-gapping) efsanesi. |
| 5 | o Hafta 5: OT İletişim Protokolü Zafiyetleri: Modbus, DNP3 ve Profinet'in güvenlik eksiklikleri ve risk mitigasyonu. |
| 6 | o Hafta 6: Endüstriyel Sistemler için Siber Risk Analizi metodolojileri ve zafiyet tarama. |
| 7 | o Hafta 7: Ara Sınav. |
| 8 | o Hafta 8: Tehdit Algılama: OT ağlarında Saldırı Tespit Sistemleri (IDS) ve anomali tespiti. |
| 9 | o Hafta 9: Olaylara Müdahale (Incident Response) ve Felaket Kurtarma (Disaster Recovery) süreçleri. |

| Hafta | Konu Başlıkları |
|---|---|
| 10 | o Hafta 10: İş Sürekliliği Planlaması (Business Continuity Planning - BCP): Kriz anında manuel operasyonlara dönüş senaryoları. |
| 11 | o Hafta 11: Tedarik Zinciri Siber Güvenliği: Üçüncü parti satıcı riskleri, donanım truva atları ve sahte (counterfeit) bileşenler. |
| 12 | o Hafta 12: Üretimde Sıfır Güven (Zero Trust) Mimarisi: Kimlik doğrulama, erişim kontrolü ve en az yetki prensibi. |
| 13 | o Hafta 13: Uluslararası Standartlar ve Uyumluluk: IEC 62443 endüstriyel güvenlik standardı ve NIST Siber Güvenlik Çerçevesi (CSF). |
| 14 | o Hafta 14: Siber-Fiziksel Dayanıklılık (Resilience) Mühendisliği: Sistem mimarisini şokları emecek ve hızlı iyileşecek şekilde tasarlama (Vaka analizleri). |